

Remarks

Reconsideration of this Application is respectfully requested.

Upon entry of the foregoing amendment, claims 1-39 are pending in the application, with 1, 17, and 33 being the independent claims. Claims 1-6, 9, 11, 13, 16, 17, 25, 28, 33-37, and 39 are amended for clarification. Support for these amendments is found in paragraphs [0028]-[0031], [0052]-[0055], [0058], and [0060] of the specification. Dependent claim 16 is amended to clarify what electronic data is secured by the access control management of claim 1. Amendments to claim 16 are supported by paragraphs [0024]-[0026] of the specification. All claim amendments are supported by the specification and have not been made to overcome prior art. These changes are believed to introduce no new matter, and their entry is respectfully requested.

Based on the above amendment and the following remarks, Applicant respectfully requests that the Examiner reconsider all outstanding objections and rejections and that they be withdrawn.

Rejections under 35 U.S.C. § 102

On page 2 of the Office Action, claims 1-37 and 39 stand allegedly rejected under 35 U.S.C. § 102(e) over US patent 6,253,193 to Ginter (US 6,253,193) ("Ginter"). Applicant respectfully traverses this rejection. Anticipation under 35 U.S.C. § 102 requires showing the presence in a single prior art reference disclosure of each and every element of the claimed invention, arranged as in the claim. See *Lindemann Maschinenfabrik GMBH v. American Hoist & Derrick*, 221 U.S.P.Q. 481, 485 (Fed. Cir. 1984).

Claims 1 and 33

On pages 3 and 4 of the Office Action, the Examiner asserts that Ginter discloses all elements of claims 1 and 33 in Figures 17 and 18, lines 8-18 of column 45, lines 6-18 of column 59, lines 31-36 and 41-65 of column 128, lines 18-20 of column 129, lines 35-37 of column 130, and lines 59-63 of column 151. Applicant has examined the above cited figures and passages in Ginter and submits that they can not reasonably be interpreted as disclosing or teaching all of the features from Applicant's amended claims 1 and 33.

Applicant respectfully submits that Ginter does not describe each and every element as set forth in amended claims 1 and 33. For example, claim 1 as amended recites a system for providing access control management to electronic data wherein the system comprises a module that generates a secured file including a header comprising a plurality of sets of encrypted security information corresponding to a respective one of a plurality of groups of users and generates an encrypted data portion encrypted with a plurality of file keys, each of the file keys corresponding to each of the sets, wherein the header is associated with the encrypted data portion. Claim 1 further recites that the system includes a module that obtains a respective one of the file keys associated with a corresponding one of the plurality of groups and decrypts the set of the respective one of a plurality of sets of encrypted security information associated with the respective one of the groups to allow access by the respective one of the groups.

Amended claim 33 recites a method for generating an electronic data in a format that provides restricted access to the electronic data where the method includes obtaining a file key, encrypting the data with the file key according to a predetermined cipher to

produce an encrypted data portion. Claim 33 as amended further recites that the method for generating and formatting the electronic data integrates a header with a plurality of sets of encrypted security information with the encrypted data portion to generate a secured file wherein the encrypted security information includes the file key and access rules to control access to the data in the file. Claim 33 also recites that each set of the plurality of sets of encrypted security information is associated with a corresponding one of a plurality of groups of users.

Applicant is unable to identify in Ginter any teaching of including a plurality of sets of encrypted security information corresponding to a respective one of a plurality of groups of users in the header of a secured electronic document as recited in claims 1 and 33. The encrypted security information in the header recited in claim 1 includes access rules that determine which users can access the electronic document, the user privileges for the document, and a file key used to access the document (paragraph [0052]). Applicant has reviewed the cited figures and passages of Ginter cited by the Examiner and submits that Ginter does not teach or suggest including a plurality of sets of security information with access rules in an encrypted header. Although Ginter may disclose a “logical object structure” that “includes a public (or unencrypted) header 802 that identifies the object and may also identify one or more owners of rights in the object and/or one or more distributors of the object” and a “private (or encrypted) header” which may “include a part or all of the information in the public header” and can “include additional data for validating and identifying the object 300 when a user attempts to register as a user of the object” (Ginter, col. 128, lns. 10-19), Ginter does not teach or suggest that encrypted security information includes a file key and access rules

to control access to the data in the file are encrypted in the header as recited in claims 1 and 33. Ginter's private or encrypted header includes data for validating and identifying the logical *object* and not *user* access rules (Emphasis added) (Ginter, col. 128, lns. 17-19). Validation and identification of a *data object* in Ginter is not analogous to using a plurality of sets of encrypted security information comprising file keys and access rules to control and allow access to *data* in a file by a plurality of users or groups as recited in amended claims 1 and 33 (Emphasis added).

While Figures 17 and 18 of Ginter may depict a logical object structure with headers, content data blocks, and permissions records with keys; these figures and their corresponding descriptions in columns 128-130 do not teach or suggest an electronic data format with a plurality of sets of security information in an encrypted header and an encrypted data portion which can be accessed using file keys contained within the header as recited in amended claims 1 and 33 (Ginter, col., 128, lns. 41-65, col. 130, lns. 13-40).

Although Ginter states that "permissions records *may* specify a user's rights to use, distribute and/or administer a container and its content, and *may* specify requirements to be applied by *budgets* and other methods" (Emphasis added) (Ginter, col. 59, lns. 6-16), Ginter's permissions records contain "*optional* control information" (Ginter, col. 26, lns. 3-7) and "*may* also contain security related information such as scrambling and descrambling keys" (Emphasis added) (Ginter, col., 59, lns. 16-18), but Ginter's permissions records do not control restricted access to electronic data in secured files as the access rules recited in claim 33 do. The access rules contained within the encrypted security information in Applicant's header are not the "optional rights records", "optional control sets", or "optional method records" disclosed by Ginter

(Ginter, col., 149, lns. 31-34). Ginter's permissions records are used to specify budgetary requirements and other budget information (Ginter, col. 59, lns. 14-16, col. 130, lns. 63-67, col. 132, lns. 55-65), and are not analogous to the access rules contained within a plurality of sets of encrypted security information which is associated with a corresponding one of a plurality of groups of users as recited in claim 33. In contrast, Applicant's access rules control how, when, and where a secured document can be accessed in addition to regulating which user(s) can access the documents (paragraph [0052], Figure 2.A). Applicant is unable to identify in Ginter a teaching of using permission records to control and restrict access to electronic data in secured files as recited in claim 33. Applicant is also unable to identify in Ginter use of permissions records to determine who can access a secured document while also regulating how, when, and where the secured document is used as recited in claim 33 and as disclosed in paragraph 52 of Applicant's specification.

While Ginter may disclose optional use of a single file key within key blocks of a permissions record to decrypt individual data blocks (Ginter, col. 128, lns. 45-65), Ginter does not teach or suggest using a plurality of file keys, each corresponding to sets of encrypted security information, to decrypt headers of secured electronic documents as recited in claims 1 and 33.

Also, at least based on their respective dependencies to claim 1, claims 2, 3, 10, 15, 16, and 39 should be found allowable, as well as for their additional respective distinguishing features. Similarly, based on their respective dependencies to claim 33, claims 34 and 38 should be found allowable, as well as for their additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claim 17

On page 4 of the Office Action, the Examiner asserts that Ginter discloses all elements of claim 17. Applicant respectfully submits that Ginter does not describe each and every element as set forth in amended claim 17. For example claim 17 recites a system for providing access control management to electronic data wherein the electronic data comprises: a header including an encrypted file key and a rule block having N encrypted segments, each of the N encrypted segments including a set of access rules facilitating the restricted access to a file including the electronic data, wherein $N \geq 1$ and an encrypted data portion including the electronic data encrypted according to a predetermined cipher. Claim 17 further recites that the header is associated with the encrypted data portion, and that the file key can be retrieved to decrypt the encrypted data portion only when the access rules in one of the N encrypted segments are measured successfully against access privileges associated with a group of designated users accessing the secured file.

Although Ginter discloses that permissions records may specify requirements to be applied by budgets and may specify user rights to use, distribute and/or administer a container and its content (Ginter, col. 59, lns. 6-16), Ginter does not teach or suggest using a set of access rules to facilitate restricted access to a file as recited in claim 17. Ginter's permissions records may contain security related information such as scrambling and descrambling keys and "optional control information" (Ginter, col. 26, lns. 3-7, col.,

59, Ins. 16-18), but are not equivalent to Applicant's access rules recited in claim 17. Ginter's permission records containing "optional rights records", "optional control sets" and "optional method records" (Ginter, col., 149, Ins. 31-34) are not analogous to the rule block having N encrypted segments where each of the N encrypted segments includes a set of access rules that facilitate restricted access recited in claim 17. Ginter's permissions records are used to specify budgetary requirements and budget information (Ginter, col. 59, Ins. 14-16, col. 130, Ins. 63-67, col. 132, Ins. 55-65), and are not analogous to the access rules contained within encrypted segments in a rule block as recited in claim 17. In contrast, the access rules recited in claim 17 control how, when, and where a secured document can be accessed in addition to regulating which user(s) can access the documents (paragraph [0052], Figure 2.A). Applicant is unable to identify in Ginter a teaching of using permission records to determine who can access a secured document while also regulating how, when, and where the secured document is used as recited in claim 17 and as disclosed in paragraph 52 of Applicant's specification.

Also, at least based on their respective dependencies to claim 17, claims 18 and 19 should be found allowable, as well as for their additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claim 2

On page 5 of the Office Action, the Examiner asserts that Ginter discloses all elements of claim 2. Applicant respectfully submits that Ginter does not describe each and every element as set forth in amended claim 2. For example claim 2 as amended recites the system to provide access control management to electronic data from claim 1 wherein the plurality of sets of encrypted security information in the header of the secured file facilitates the restricted access to the file.

Ginter may disclose that separate permissions records can contain one or more keys (Ginter, col. 130, lns. 35-37) used to decrypt body information in a container object (Ginter, col. 151, lns. 56-67), but Ginter does not suggest using a plurality of sets of encrypted security information in the header of the secured file to facilitate restricting access to the file as recited in Applicant's claim 2. Although Ginter discloses that a logical object structure may include an encrypted, private body containing or referencing a set of methods such as programs or procedures that control use and distribution of a container object (Ginter, col. 128, lns. 25-40), it further teaches that the private body is located *outside* of the public, unencrypted header and the private, encrypted header (Emphasis added) (Ginter, col. 128, lns. 10-20). Ginter does not teach or suggest that a plurality of sets of encrypted security information is contained within the header of a secured file as recited in amended claim 2.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejection of this claim, and find it allowable over the applied reference.

Claims 3 and 35

On pages 5 and 6 of the Office Action, the Examiner asserts that Ginter discloses all elements of claims 3 and 35. Applicant respectfully submits that Ginter does not describe each and every element as set forth in amended claims 3 and 35. For example amended claims 3 and 35 recite a system and method, respectively, for providing access control management to electronic data from claims 1 and 34, respectively, wherein the plurality of sets of security information is encrypted with a key from the plurality of file keys associated with one of a plurality of groups of users.

Ginter may disclose that separate permissions records can contain one or more keys (Ginter, col. 130, lns. 35-37) used to decrypt body information in a container object (Ginter, col. 151, lns. 56-67), but Ginter does not teach using a plurality of sets of file keys associated with one of a plurality of groups of users to encrypt a plurality of sets of security information in a header of a secured document as recited in claims 3 and 35.

Also, at least based on its dependency to claim 3, claim 4 should be found allowable, as well as for its additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claims 4 and 36

On page 6 of the Office Action, the Examiner asserts that Ginter discloses all elements of claims 4 and 36. Applicant respectfully submits that Ginter does not describe each and every element as set forth in amended claims 4 and 36. For example

amended claims 4 and 36 recite a system and method, respectively, for providing access control management to electronic data from claims 3 and 34, respectively, wherein the corresponding one of a plurality of groups of users of users includes one or of human users, software agents, and devices; and wherein the users are granted access privileges to access the secured file.

Although Ginter discloses people as users and end-users (Ginter, col. 53, lns. 8-10, col. 255, lns. 6-13, Figures 1 and 2) and a Virtual Distribution Environment (VDE) involving "at least one human user" (Ginter, col. 245, lns. 41-43), Applicant is unable to identify in Ginter a teaching of a software agent or device, or plurality of software agents or devices that are users who are granted access privileges to secured files.

Also, at least based on its dependency to claim 4, claim 5 should be found allowable, as well as for its additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claim 5

On page 6 of the Office Action, the Examiner asserts that Ginter discloses all elements of claim 5. Applicant respectfully submits that Ginter does not describe each and every element as set forth in amended claim 5. For example amended claim 5 recites the system to provide access control management to electronic data from claim 4 wherein the plurality of sets of encrypted security information comprises one of the plurality of file keys and access rules to restrict access to the file.

Although Ginter may disclose encrypting a “container” body with “private body keys” and data blocks with “content keys” from permissions records (Ginter, col., 130, lns. 35-40), Ginter does not teach or suggest encrypting file keys within a plurality of sets of encrypted security information where the sets also contain access rules as recited in claim 5. Ginter may disclose that container objects include private bodies with programs or procedures that control object use (Ginter, col., 128, lns. 25-28), but Ginter does not teach or suggest that encrypted sets of security information comprises one of a plurality of file keys and access rules to restrict access to the file as recited in Applicant's claim 5.

Also, at least based on its dependency to claim 5, claim 6 should be found allowable, as well as for its additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claims 7 and 26

On page 6 of the Office Action, the Examiner asserts that Ginter discloses all elements of claims 7 and 26. Applicant respectfully submits that Ginter does not describe each and every element as set forth in claims 7 and 26. For example claims 7 and 26 recite the method and system from claims 7 and 25, respectively, for providing access control management to electronic data wherein access rules are expressed in a markup language. Although Ginter may disclose expressing data description element (DTD) information in a languages such as the SGML markup language and English

(Ginter, col. 141, lns. 34-41), Ginter does not suggest that access rules contained within an encrypted security portion of electronic data are coded in a markup language as recited in Applicant's claims 7 and 26. Ginter discloses that data description elements (DTDs) are stored within load modules which in turn include public (unencrypted) and private (encrypted) headers (Ginter, col. 140, lns. 7-14, Figure 23). Ginter discloses that permissions records (PERCs) *control* load modules (Emphasis added) (Ginter, col. 139, lns. 60-66), and that PERCs are distinct from load modules (Ginter, Figure 16). Ginter also discloses that DTDs optionally written in SGML are separate from the private and public header of a data container (Ginter, col. 141, lns. 34-41, Figure 23). Applicant submits that load modules with DTDs stored within are not analogous to access rules recited in claims 7 and 26. Applicant is unable to find any teaching in Ginter of expressing permissions records or access rules in a markup language as recited in Applicant's claims 7 and 26.

Also, at least based on their respective dependencies to claims 7 and 26, claims 8-9 and 27-28 should be found allowable, as well as for its additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claims 5-7, 13, 17, 24, 26, 30, 31, and 37

On pages 4, 6-7, and 9-11 of the Office Action, the Examiner asserts that Ginter discloses all elements of claims 5-7, 13, 17, 24, 26, 30, 31, and 37. Applicant

respectfully submits that Ginter does not describe each and every element as set forth in claims 5-7, 13, 17, 24, 26, 30, 31, and 37. The access rules recited in claims 5-7, 13, 17, 24, 26, 30, 31, and 37 are used to determine how, when, and where a secured document can be accessed in addition to controlling which users can access documents (paragraph [0052], Figure 2.A). As discussed above, Ginter's permissions records do not control how, where, and when a secured electronic document can be accessed in addition to determining who can access the document. Applicant therefore submits that Ginter does not teach or suggest access rules which impose four types of secured document access control as recited in claims 5-7, 13, 17, 24, 26, 30, 31, and 37.

Also, at least based on their respective dependencies to claims 7, 13, 17, 24, 26, and 30, claims 8-9, 14, 18-19, 25, 27-28, and 31 should be found allowable, as well as for their additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claim 11

On page 7 of the Office Action, the Examiner asserts that Ginter discloses all elements of claim 11 in lines 63-66 of column 137. Applicant respectfully submits that Ginter does not describe each and every element as set forth in amended claim 11. For example claim 11 as amended recites the system to provide access control management to electronic data from claim 10 wherein each of the plurality of sets of encrypted security information comprises a flag to the application that the secured file being

accessed can not be accessed as it is normally accessed. Applicant has examined lines 63-66 of column 137 of Ginter and is unable to identify any disclosure or teaching of plurality of sets of encrypted security information including flags to an application to indicate that a secured file being accessed can not be accessed as it is normally is as recited in Applicant's claim 11. Although Ginter may disclose setting or using an array of data fields or flags to indicate how data is used over time (Ginter, col. 147, lns. 40-47, Figure 25C), Applicant is unable to identify in Ginter a teaching of including or setting flags within encrypted security information so that an application is notified that a secured file cannot be accessed as it normally is accessed by the application as recited in claim 11.

Also, at least based on its dependency on claim 11, claim 12 should be found allowable, as well as for its additional respective distinguishing features.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claims 18 and 22

On page 8 of the Office Action, the Examiner asserts that Ginter discloses all elements of claims 18 and 22 in line 31 of column 128 which reads:

“Methods 1000 perform the basic function of defining what users (including, where appropriate, distributors, client administrators, etc.), can and cannot do with an object.”

Applicant respectfully submits that Ginter does not teach each and every element as set forth in amended claims 18 and 22. For example claims 18 and 22 as amended

recite, respectively, the systems to provide access control management to electronic data from claims 17 and 20 wherein the header further comprises a user block having user information identifying who can access the secured file. While Ginter may disclose using *methods* that function to determine who can access an object (Emphasis added) (Ginter, col. 128, lns. 30-33), Ginter does not teach or suggest storing a user block within an encrypted header of a secured document that identifies which users are allowed to access the file as recited in claims 18 and 22. Ginter's methods are "programs or procedures" stored or referenced in a container body (Ginter, col. 128, lns. 25-28) and are not analogous to Applicant's user block information stored in an encrypted header as recited in claims 18 and 22.

Also, at least based on its dependency on claim 18, claims 20 should be found allowable, as well as for its additional respective distinguishing features. Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Claims 21-24, 29, 30, and 32

On pages 9-11 of the Office Action, the Examiner asserts that Ginter discloses all elements of claims 21-24, 29, 30, and 32. Applicant respectfully submits that Ginter does not describe each and every element as set forth in dependent claims 21-24, 29, 30, and 32.

Claims 21-24, 29, 30, and 32 all recite the user block feature as set forth in claims 18 and 22, and the user block feature not described by Ginter. For example, claim 21 recites the system to provide access control management to electronic data from claim 20

wherein each of the N encrypted segments of the user block corresponds to one of the N encrypted segments of the rule block. As discussed above, Ginter does not teach each and every element of claim 21 because Ginter does not teach or suggest storing N encrypted segments of a user block identifying who can access the secured file within an encrypted header of a secured document. Similarly, as the user block feature is not taught or suggested by Ginter, Ginter also does not teach each and every element of claims 22-24, 29, 30, and 32.

Also, at least based on its dependency on claim 24, claim 25 as amended should be found allowable, as well as for its additional respective distinguishing features. Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of these claims, and find them allowable over the applied reference.

Rejections under 35 U.S.C. § 103

Claim 38 is rejected under 35 U.S.C. § 103(a) as allegedly being unpatentable over Ginter in view of US patent to Folmsbee (US 6,308,256) ("Folmsbee"). Applicant respectfully traverses this rejection. Claim 38 recites a combination of features that are not found in the applied references. For example, claim 38 recites the electronic document formatting method from claim 33 wherein obtaining the file key comprises: generating the file key from the predetermined cipher if the secured file is newly generated; retrieving the file key from a memory store if the secured file is being stored in a storage place; and deleting the file key from a memory store as soon as the secured file is stored in the storage place.

On page 12 of the Office Action, the Examiner acknowledges that Ginter is silent about retrieving a file key from a memory store and deleting the key from a memory store as soon as the secured file is stored in the storage place as recited in claim 38. The Examiner asserts that this deficiency is cured by line 4 of column 16 of Folmsbee, which reads:

“The key expiry event could be any convenient event, such as time of usage, real time or number of uses.”

Applicant has examined line 4 of column 16 of Folmsbee and submits that it cannot be reasonably interpreted to teach or suggest the above recited features of claim 38. Folmsbee is concerned with the specific problems associated with preventing unauthorized use of software that is transferred in a communications network (Folmsbee, col. 1, lns. 28-36). Folmsbee seeks to prevent unauthorized use of programs not by encrypting programs or having program data “scrambled by a standard microprocessor,” but by using “a microprocessor that is being scrambled to process standard data” (Folmsbee, col. 16, lns. 24-27). Folmsbee may disclose that keys can *expire* upon occurrence of a “key expiry event” and that key expiry events can be events such as the amount of time a software program is used or the number of times a software program has been used (Folmsbee, col., 16, lns. 2-4, Figure 12), but Folmsbee does not teach or suggest that file encryption keys are *deleted* from memory stores as soon as a secured file is stored as recited in Applicant's claim 38 (Emphasis added). Folmsbee's expired software keys are not deleted upon their expiration (Folmsbee, col. 16, lns. 10-11, Figure 12) and are not deleted from memory stores as soon as associated secured files are stored as recited in Applicant's claim 38. Applicant is unable to identify in Folmsbee any

teaching of deleting a file key and submits that Folmsbee is limited to terminating a program if the associated key has expired (Folmsbee, col. 16, lns. 10-16, Figure 12).

Applicant further submits that the stored keys in Folmsbee are used to prevent unauthorized execution of software programs by restricting their execution to a microprocessor (Folmsbee, col. 1, lns. 28-36, col. 2, lns. 40-65) and are not analogous to the generated file keys from the predetermined cipher which control electronic data access as recited in Applicant's claim 38.

Accordingly, Applicant respectfully request this rejection be removed and this claim be passed to allowance.

Also, Applicant submits that any use by the Examiner to apply piecemeal parts of Folmsbee to Ginter to cure the deficiencies in Ginter would destroy the teaching of both of these references by making the systems/methods of operation unsatisfactory for their intended purposes and/or change the systems/principles of operation. See M.P.E.P. § 2143.01(V) and (VI). For example, as Ginter discloses that "users can also benefit from a transparent interaction with many of the capabilities" of the Virtual Distribution Environment (VDE) (Ginter, col. 34, lns. 49-51) and Folmsbee's user notifications, warnings, and program termination features (Folmsbee, col. 16, lns. 6-13, Figure 12) interfere with this transparency, adding Folmsbee to Ginter destroys Ginter's user transparency feature. Similarly, as Folmsbee "is not about data that is being scrambled by a standard microprocessor" (Folmsbee, col. 16, lns. 24-25), adding Ginter's "scrambling and descrambling keys" (Ginter, col., 59, lns. 16-18) for encryption of VDE data containers to Folmsbee destroys Folmsbee's feature of preventing unauthorized program execution without scrambling or encrypting the program data.

Accordingly, Applicant respectfully requests that the Examiner reconsider and withdraw the rejections of this claim, and find it allowable over the applied references.

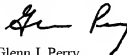
Conclusion

All of the stated grounds of objection and rejection have been properly traversed, accommodated, or rendered moot. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding objections and rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment and Reply is respectfully requested.

Respectfully submitted,

STERNE, KESSLER, GOLDSTEIN & FOX P.L.L.C.



Glenn J. Perry
Attorney for Applicant
Registration No. 28,458

Date: July 11, 2007

1100 New York Avenue, N.W.
Washington, D.C. 20005-3934
(202) 371-2600

690613_4.DOC